Bancos e Internet

Este curso busca responder las siguientes tres preguntas:

- ¿Qué hacen los bancos para protegerte?
- ¿Que debes hacer tú para protegerte?
- ¿Cuales son los bancos más seguros? Comparativa de páginas web de bancos.

La presente publicación pertenece a su autora Isabel Cuéllar Hernández y está bajo una licencia Reconocimiento-Nocomercial-CompartirIgual 3.0 España de Creative Commons, y por ello está permitido copiar, distribuir y comunicar públicamente esta obra bajo las condiciones siguientes:

• Reconocimiento: El contenido de este informe se puede reproducir total o parcialmente por terceros, citando su procedencia y haciendo referencia expresa su autora Isabel Cuéllar Hernández. Dicho reconocimiento no podrá en ningún caso sugerir que su autora presta apoyo a dicho tercero o apoya el uso que hace de su obra.

• Uso No Comercial: El material original y los trabajos derivados pueden ser distribuidos, copiados y exhibidos mientras su uso no tenga fines comerciales.

• Compartir bajo la misma licencia: Si transforma o modifica esta obra para crear una obra derivada, sólo puede distribuir la obra resultante bajo la misma licencia.

Un resumen de la licencia se puede consultar en http://creativecommons.org/licenses/by-nc-sa/3.0/es/

El texto legal de la licencia se puede consultar en http://creativecommons.org/licenses/by-nc-sa/3.0/legalcode

- # ¿Qué hacen los bancos para protegerte?

Tu banco, encripta la conversación → https → para que nadie pueda conseguir ninguna información útil de la conversación entre tu y tu banco.

Tu banco tiene un certificado para que puedas confirmar que estas entrando *en la página web de tu banco*.

Tu banco, te ofrece un teclado virtual → para que ninugún virus pueda capturar tus contraseñas.

Tu banco, te ofrece una contraseña diferente para acceder que para firmar.
Mejor si es una tarjeta de coordenadas, pues mucho más dificil de capturar completamente.

Tu banco te permite utilizar autenticación de dos factores, es decir, algo que sabes (tus contraseñas) y algo que tienes (mensajes de confirmación al móvil).

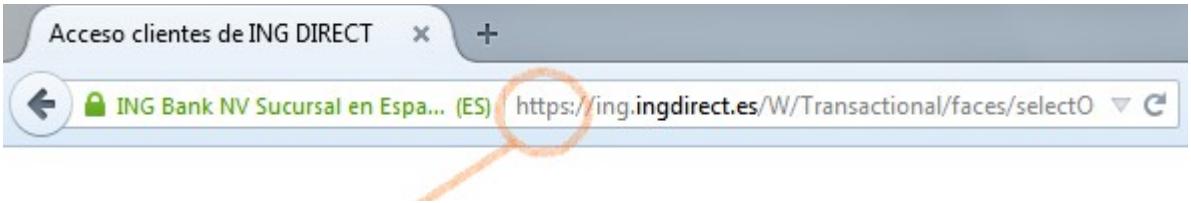
Tu banco te desconectará automáticamente de su página web si no detectecta actividad en cierto periodo de tiempo (5, 10 minutos).

Tu banco te ofrece el servicio de avisarte (con un mensaje al móvil o email) cada vez que se realiza un movimiento de dinero en tus cuentas.

Tu banco te enseña como usar sus servicios de la manera más segura.

> Nunca debes acceder al banco por medio de un enlace en un e-mail o página web que no sea de absoluta confianza. En vez de eso, teclea la dirección en el navegador.
>
> Nunca se te solicitará, ni por teléfono ni por Internet, la **contraseña** de seguridad al **completo**, ni **todos** los valores de la tarjeta de **coordenadas**.

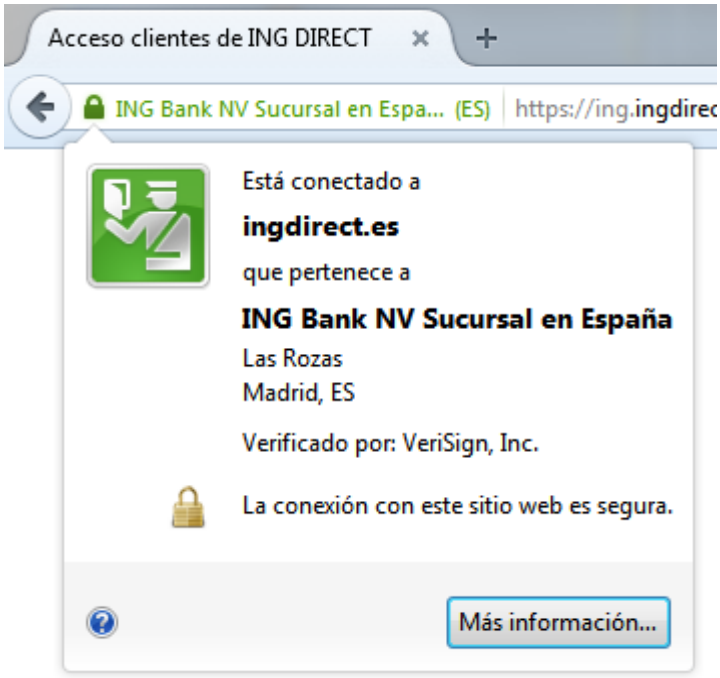
Tu banco, encripta la conversación → https → para que nadie pueda conseguir ninguna información útil de la conversación entre tú y tu banco.



Tu banco tiene un certificado para que puedas confirmar que estas entrando ***en la página web de tu banco***

Se puede saber si una página tiene un certificado válido, buscando el dibujo de un candado.

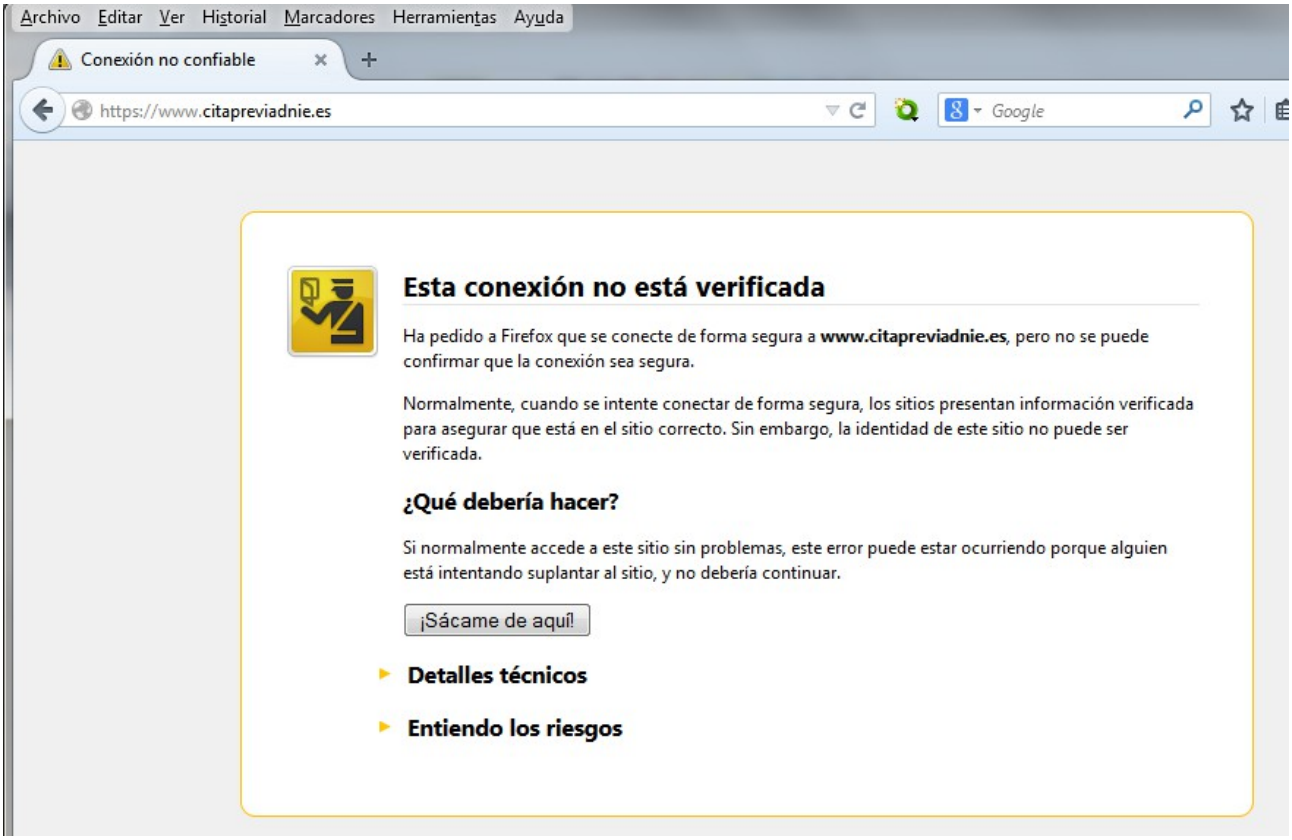
Ejemplo:



Este certificado se puede ver en la página de *Acceso para clientes* de Ing Direct

Está autenticado por la empresa VeriSign, la cual informa que la página web **efectivamente** pertenece a Ing Direct.

Si ves esto, significa que el certificado no esta firmado por ninguna entidad que sea reconocida por el navegador.

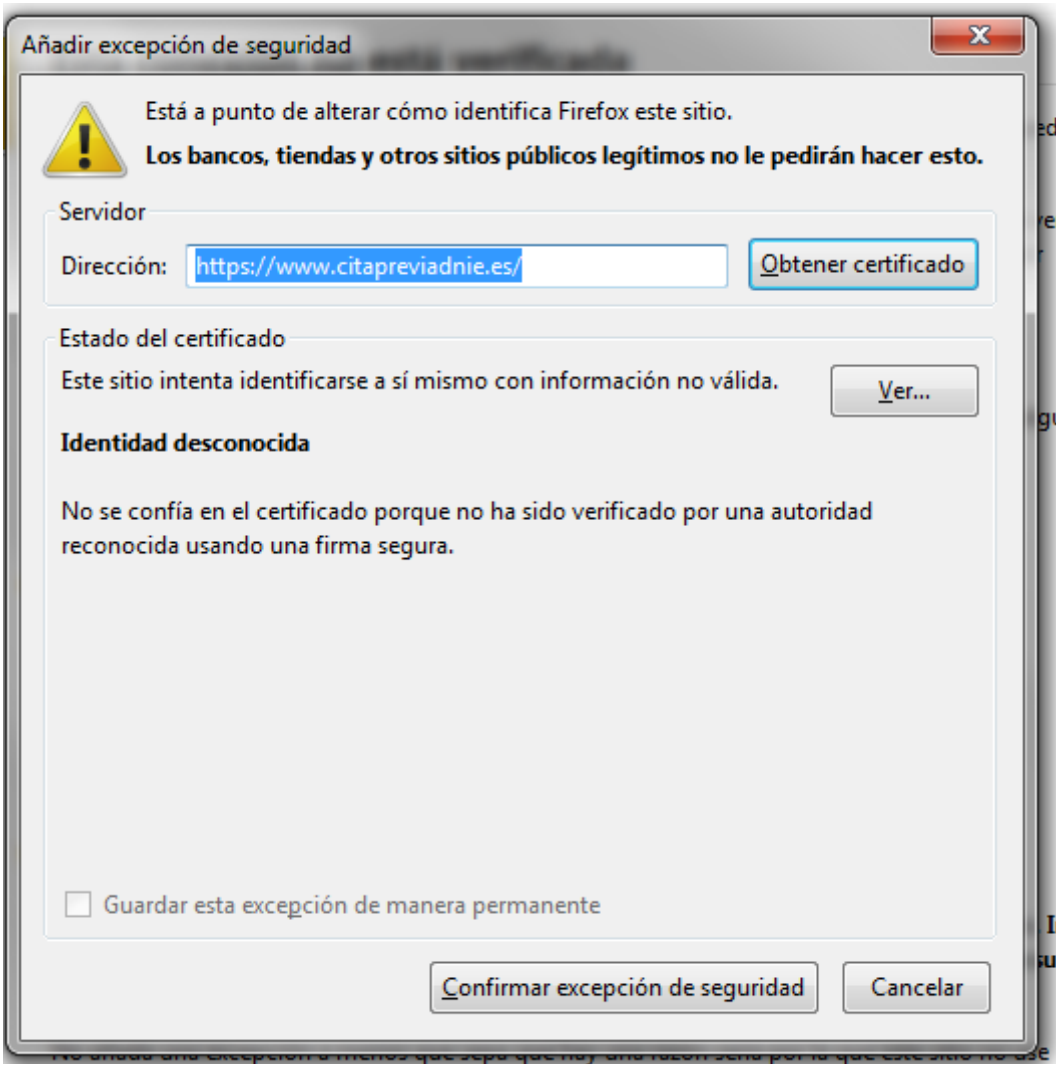


Eso puede ser común para páginas de la Administración Pública (hacienda, seguridad social, policia, …), porque la entidad que los firma, suele ser la misma Administración, que no está recocida por defecto en los navegadores.

Pero no es muy habitual en paginas de bancos. Si no aparece el dibujo de un candado en la barra de direcciones, desconfía.

Solo si estás seguro de que la página a la que quieres acceder es segura (por ejemplo, hacienda, seguridad social, policia, ...)

Haz click en “Entiendo los riesgos” y “Añadir excepción”. Y por último en “Confirmar excepción de seguridad”.



Tu banco, te ofrece un teclado virtual → para que ningún virus pueda capturar tus contraseñas.

Como hemos visto, la información entre tu y tu banco está encriptada, por lo tanto nadie que escuche puede capturar los números de tus contraseñas.

Pero, puede pasar, que tu ordenador tenga un tipo especial de virus llamado *keylogger,* que detecta las pulsaciones del teclado.

Por ello, es muy importante que se uses un teclado virtual, que sustituye las pulsaciones del teclado por clicks de ratón.

Otro detalle importante que se puede ver en la imagen de arriba, es el aviso de que el banco nunca te pedirá tu clave de acceso completa.

Esto se hace así para evitar que un atacante pueda conseguir tu clave completa.

Tu banco, te ofrece una contraseña diferente para acceder que para firmar.

Ya sabes que es útil tener contraseñas distintas para distintos usos. Por ejemplo, una contraseña para acceder y otra, diferente, para firmar y confirmar operaciones.

Sin embargo, es aún más seguro, usar una tarjeta de coordenadas en vez de una contraseña de firma.

La Tarjeta de Coordenadas es una tarjeta de plástico, del tamaño de una tarjeta de crédito, que contiene una matriz o serie de números impresos.

Al solicitar una transacción protegida por Tarjeta de Coordenadas el sistema requerirá el número que se encuentra impreso en alguna celda. Por ejemplo, se nos solicitará la coordenada 12, y tendremos que introducir 450.

El banco nunca nos solicitará todas las coordenadas juntas de la tarjeta de coordenadas y nunca por e-mail o teléfono.
Y en general no se solicitan más de 1 o 2 valores por operación.

Este sistema es mucho más seguro puesto que un atacante necesitaría conseguir todas las coordenadas antes de poder confirmar transferencias en nuestro nombre.

Tu banco te permite utilizar autenticación de dos factores, es decir, algo que sabes (tus contraseñas) y algo que tienes (mensajes de confirmación al móvil)

No se lo vamos a poner tan fácil a un atacante, ¿verdad?

Además de usar contraseñas y la tarjeta de coordenadas, le pedimos al banco que,cada vez que vayamos a confirmar una operación, nos envie un mensaje al móvil con el número de la coordenada que necesitamos escribir para confirmar esa operación.

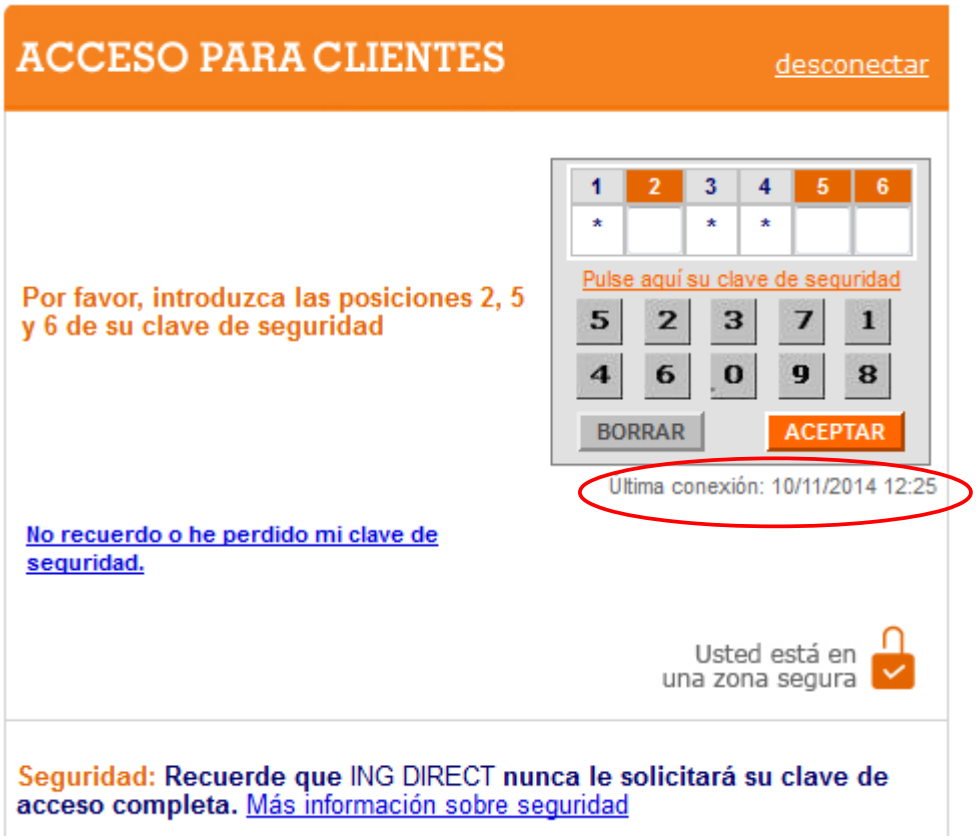
Esto se llama autenticación de dos factores.

Tu banco te desconectará automáticamente de su página web si no detectecta actividad en cierto periodo de tiempo (5, 10 minutos).

Si durante la sesión de banca virtual transcurre un periodo de tiempo en el que tu ordenador permanece inactivo, se producirá una desconexión automática.
Tu banco supone que se te ha olvidado cerrar la sesión y la cierra por ti.
Esto evita que una persona con acceso a tu ordenador (acceso físico o remoto) encuentre la sesión activa y pueda realizar algún tipo de fraude.

Acuerdate siempre de cerrar tu sesión de la forma correcta, buscando un botón o enlace “Desconectar” o “Salir”.
En caso contrario se pueden quedar restos en tu ordenador, que pueden ayudar a algún atacante.

También es recomendable que revises la última vez que te conectaste (deberia aparecer en la pantalla de inicio o en la página principal) para detectar conexiones que no has hecho tú, y poder alertar a tu banco.



Tu banco te ofrece el servicio de avisarte (con un mensaje al móvil o email) cada vez que se realiza un movimiento de dinero en tus cuentas

Por si todo demás falla, es muy importante que solicites a tu banco que te avise cada vez que se realiza un movimiento de dinero en tus cuentas.

Esto te permite tener un mayor control sobre tus cuentas y tarjetas.
Entre otros, te permite saber, desde el primer momento, si se está produciendo un robo o acto irregular en tus cuentas.
En el caso de que se produzca, lo primero que debes hacer es llamar a tu banco para que bloqueen tus cuentas, e **inmediatamente** después, denunciarlo a la **policía**.

Tu banco te debe proporcionar una manera fácil y siempre disponible de bloquear tus cuentas, si piensas que han sido comprometidas (por ejemplo, un teléfono, que aparezca en su página principal).

Esto significa que debes cambiar tus claves por unas nuevas, y para hacerlo, tu banco te debe obligar a ir a un oficina físicamente, como única forma de probar tu identidad.

Si olvidas, tus claves, también has de ir personalmente a una oficina.
O, en su defecto, tu banco te puede enviar unas claves nuevas por correo postal a tu casa. Por supuesto, el sobre no podrá estar identificado con el logo del banco, y las nuevas claves vendrán desactivadas (trendrás que activarlas contestando unas preguntas personales en la página web).

Tu banco te enseña como usar sus servicios de la manera más segura.

Tu banco es un banco que se preocupa por la seguridad si insiste, el lugares destacados, en los siguietes puntos:

Nunca debes acceder al banco por medio de un enlace en un e-mail o página web que no sea de absoluta confianza. En vez de eso, teclea la dirección en el navegador.

Nunca se te solicitará, ni por teléfono ni por internet, las **contraseñas** al **completo**, ni **todos** los valores de la tarjeta de **coordenadas**.

• ¿Que debes hacer tú para protegerte?

Mantén tu ordenador seguro

Instala un antivirus, un firewall y las actualizaciones de seguridad

Ten mucho cuidado con las páginas web que visitas, los emails que abres y los programas que descargas.

Si quieres la *absoluta* seguridad de acceder a tu banco sin virus, usa LPS Linux.

Mantén tus contraseñas seguras

Impide que sean fácilmente adivinables, evita las fechas y otra información personal tuya, que se pueda conseguir en las redes sociales.

Cámbialas periódicamente.

No dejes que los navegadores las recuerden.
No las escribas sin encriptar en ninguna parte de tu ordenador.

No uses la misma contraseña en dos sitios distintos (es decir, la misma contraseña para todas tus tarjetas, …)

Mantén tu ordenador seguro

Instala un antivirus, un firewall y las actualizaciones de seguridad

Antivirus

La eficacia de los antivirus empieza en el 90% de detección, en algunos antivirus es más alta que en otros, pero nunca llega al 100%.

Existen diferentes tipos de antivirus, algunos son gratuitos y otros son de pago, pero, en mi opinión, no es necesario escoger ningún antivirus específico para estar seguros.

Lo importante es conseguir el antivirus de forma fiable(teniendo cuidado con el software que se instala. Instalar solo de sitios oficiales. No instalar software pirata.) y mantenerlo actualizado !

Ejemplos de antivirus fáciles de usar: Microsoft Security Essentials, Avast!, Avira ...

Firewall

Exactamente igual que con los antivirus, los puntos importantes a la hora de usar un cortafuegos son que sea fácil de usar, conseguido por medios fiables y se mantenga actualizado.

Ejemplo de cortafuegos fácil de usar: Cortafuegos de Windows.

Para acceder a las opciones del cortafuegos hay que ir a Inicio -> Panel de Control -> Sistemas y Seguridad > Firewall.

Es posible habilitar o deshabilitar el cortafuegos pulsando en la opción "Activar o desactivar cortafuegos de Windows" que hay en el menú izquierdo de la ventana.

Actualizaciones de seguridad

Las actualizaciones de seguridad más importantes son tres: Java, Windows y Flash Player.

Aunque es una buena idea que aceptes la actualizaciones de seguridad de otros programas (firefox, chrome, adobe reader, ...).

Java

Es posible que tengas instalado el programa java en tu equipo y no lo necesites. Esto solo puedes comprobarlo, probando a desinstalar java y comprobando que puedes trabajar normalmente con tu equipo.

Si es así, es mucho más recomendable y más cómodo que desinstales java en vez de actualizarlo.

Para desinstalar java,

Hacer clic en *Inicio → Panel de control → Desinstalar un Programa*

En la lista de programas, seleccionar todas las versiones de java y hacer doble clic sobre cada una de ellas.

Reinicia el equipo

Windows

Pulsar en *Inicio → Todos los programas-> Windows Update*, en el panel izquierdo, pulsar en *Cambiar la configuración*.

Del desplegable de *Actualizaciones importantes*, seleccionar *Instalar actualizaciones automáticamente (recomendado)*, se marcará la opción *Permitir que todos los usuarios instalen actualizaciones en este equipo*.

Por último, hacer clic en el botón *Aceptar*

Flash Player

Hacer clic en *Inicio --> Panel de control*

Cambiar la vista de “Categorías” a “Iconos pequeños”.

Hacer doble clic en el icono de *Flash Player*. Aparece el Panel de control de Flash Player.

Hacer clic en la pestaña *Avanzado*.

Para activar la función Actualización de Flash de modo que se instalen automáticamente las actualizaciones, seleccionar la casilla *Instalar actualizaciones automáticamente si están disponibles.*

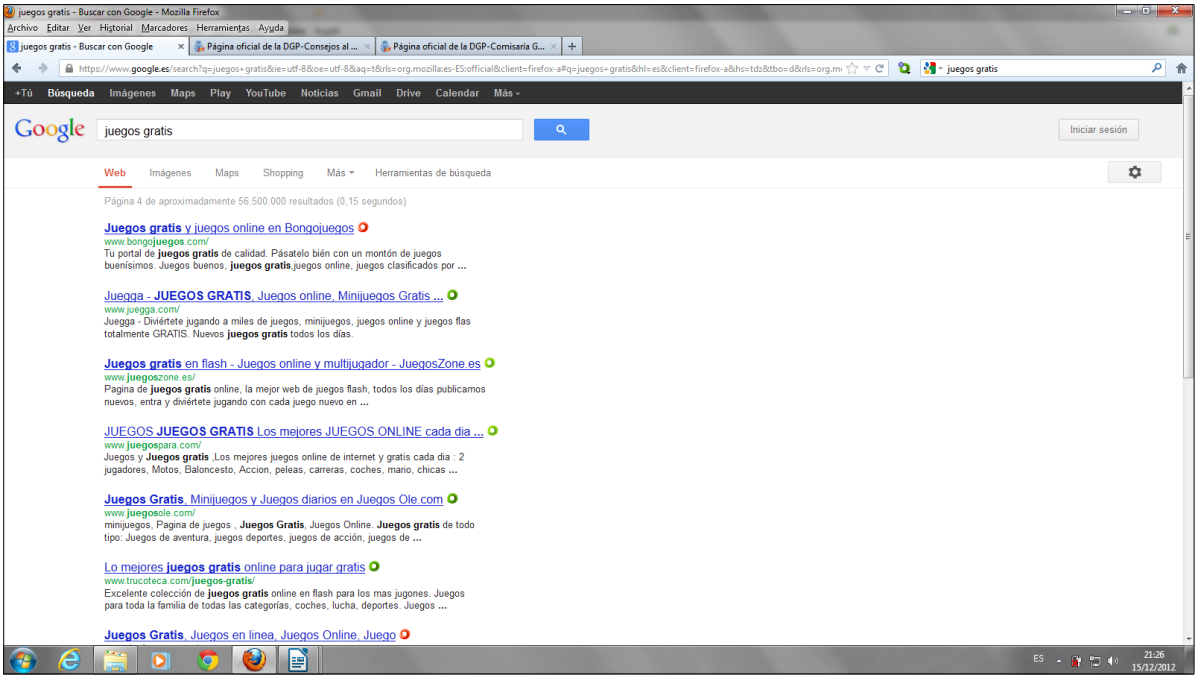
Ten mucho cuidado con las páginas web que visitas, los emails que abres y los programas que descargas.

En ningún caso instales nada que te proponga una página web o un programa que no conozcas.

Algunas extensiones para navegador pueden ayudar a detectar sitios dañinos.

Por ejemplo, WOT

(También el antivirus puede incluir herramientas que ayuden a detectar sitios dañinos)



Para instalar WOT en Firefox se debe:

Ir a Herramientas → Complementos → Obtener Complementos

Buscar WOT en el cuadro de búsqueda y hacer clic en Instalar

Para instalar WOT en Chrome se debe:

Ir a Herramientas → Extensiones → Obtener Mas Extensiones

Buscar WOT en el cuadro de búsqueda y hacer clic en Añadir a Chrome

Para instalar WOT en Internet Explorer se debe:

Ir a la página oficial de WOT, http://www.mywot.com/en/download

e instalarlo desde allí.

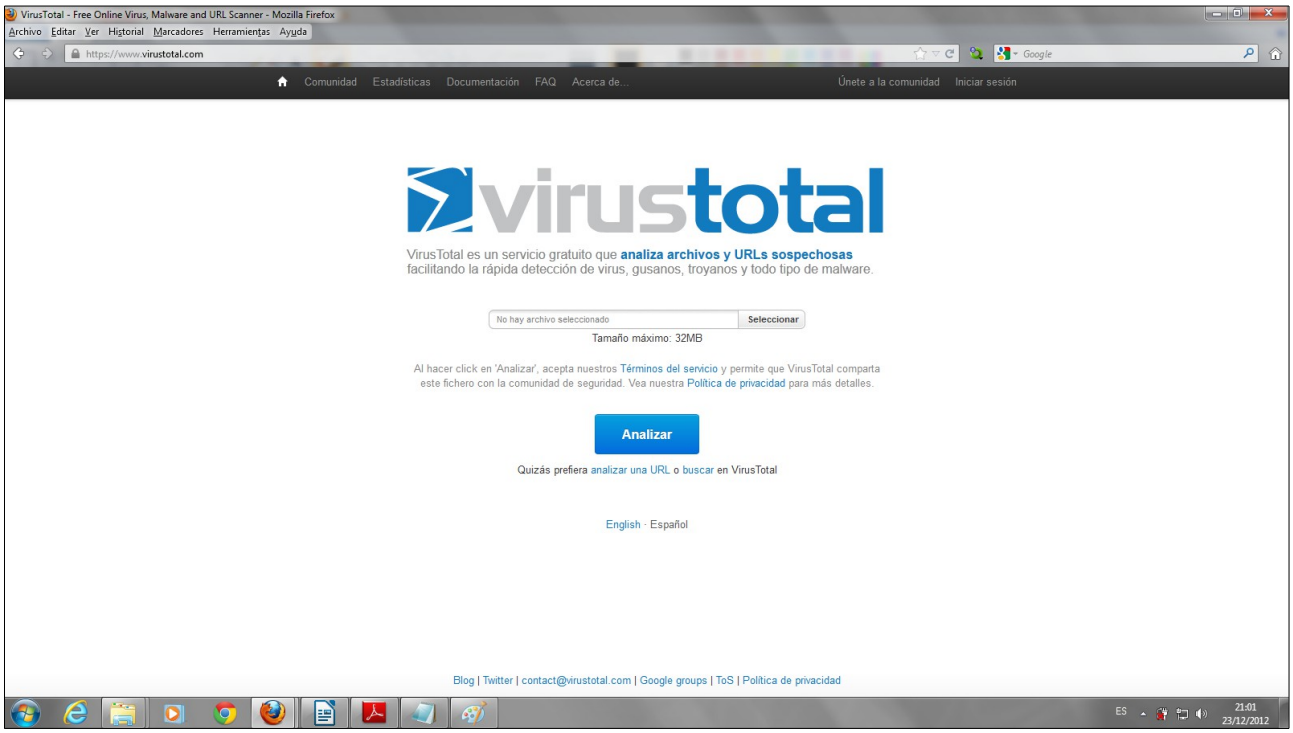
Se recomienda siempre obtener los programas o contenidos de sus respectivos sitios **oficiales**.

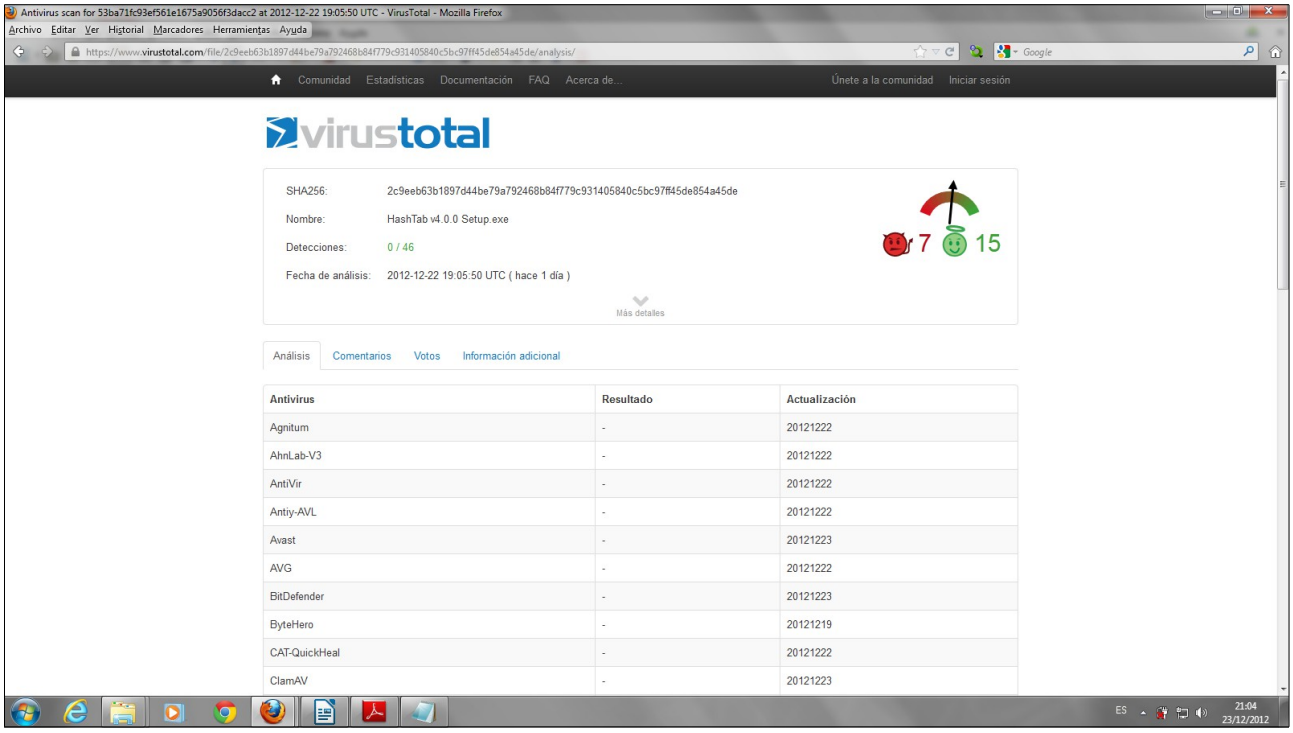
Desconfía de sitios con muchos anuncios parpadeantes como Softonic.

También se recomienda analizar los archivos descargados con un motor antivirus antes de abrirlos

Para ello, puedes usar la herramienta online Virus Total

https://www.virustotal.com/





Si quieres la seguridad de acceder a tu banco sin virus, usa LPS Linux.

Consideraciones previas

En su mayor parte, un ordenador se usa para navegar por Internet, acceder al correo electrónico y/o descargar vídeos, música o programas de utilidad.

Estas actividades pueden provocar que el equipo desde el que se realizan sea "infectado" por un virus, con consecuencias que pueden llegar a ser extremadamente perjudiciales.

Situaciones, potencialmente, de ALTO RIESGO.

Más en concreto, una actividad cada vez más cotidiana es acceder a los sitios web de los Bancos, para gestionar los recursos allí depositados.

Otra actividad habitual es pagar recibos, entradas, impuestos, etc., o incluso realizar operaciones más complejas.

Un virus potente podría hacer llegar nuestros datos identificativos (número de cuenta y contraseña, por ejemplo) a manos indeseables.

Una solución

Para evitar problemas, una excelente solución es utilizar el

sistema LPS (una distribución de Linux)

cuya fácil implementación se describe a continuación.

El sistema LPS permite acceder al banco por internet usando únicamente la información del CD donde LPS reside, una información que sabemos que está libre de virus.

Utilizando LPS evitamos la necesidad de usar la información del ordenador donde puede estar escondido un virus.

Creación de un CD de arranque con el "sistema LPS"

Previo importante: será necesario grabar un CD cada vez que esté disponible una versión nueva del "sistema LPS", para así contar con las más recientes actualizaciones de seguridad. Se recomienda hacerlo cada tres o cuatro meses.

Descarga del software necesario

Acceder a

http://www.spi.dod.mil/docs/LPS-x.x.x_public.iso (siendo x-x-x la versión)

lo que desencadenará la descarga del archivo "LPS-x.x.x_public.iso".

Guardarlo en el disco duro (se propone "C:\temp").

Grabación del "sistema LPS" en un CD

Insertar un CD en blanco en la unidad que corresponda.

Utilizando el "Explorador de Windows", acceder al archivo guardado en el paso anterior, y hacer clic en él con el botón derecho. Seleccionar "Grabar imagen de disco".

En el cuadro de diálogo que aparecerá:

- activar "Comprobar disco después de grabar", y
- hacer clic en "[Grabar]"

nota importante: al usar estos programas se deberá seleccionar la opción **"Grabación de archivos ISO (o equivalente)"**, pues si se realizara la grabación utilizando la opción "Grabación de archivos de datos (o equivalente)" no se generaría un disco de arranque, por lo que el "sistema LPS" no funcionaría.

Uso del sistema LPS

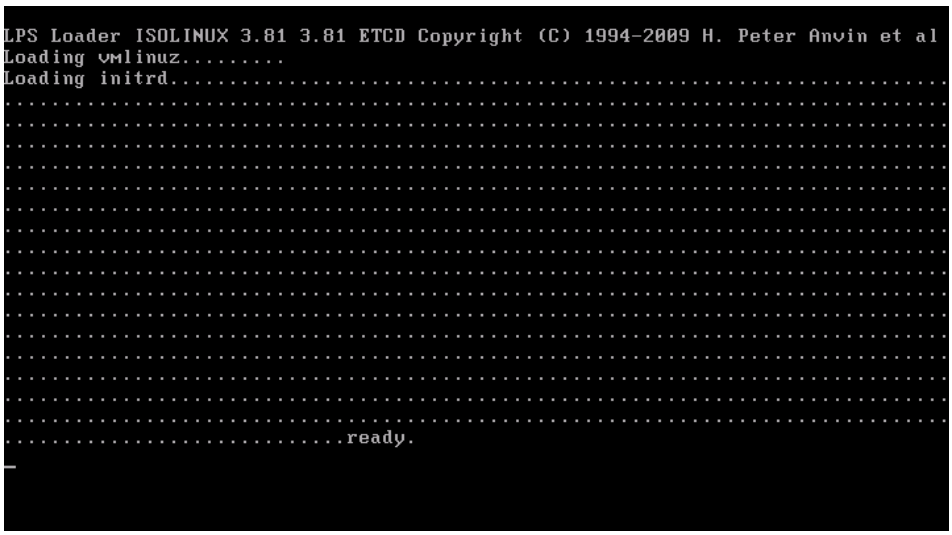
Introducir el CD recién creado en la unidad correspondiente.

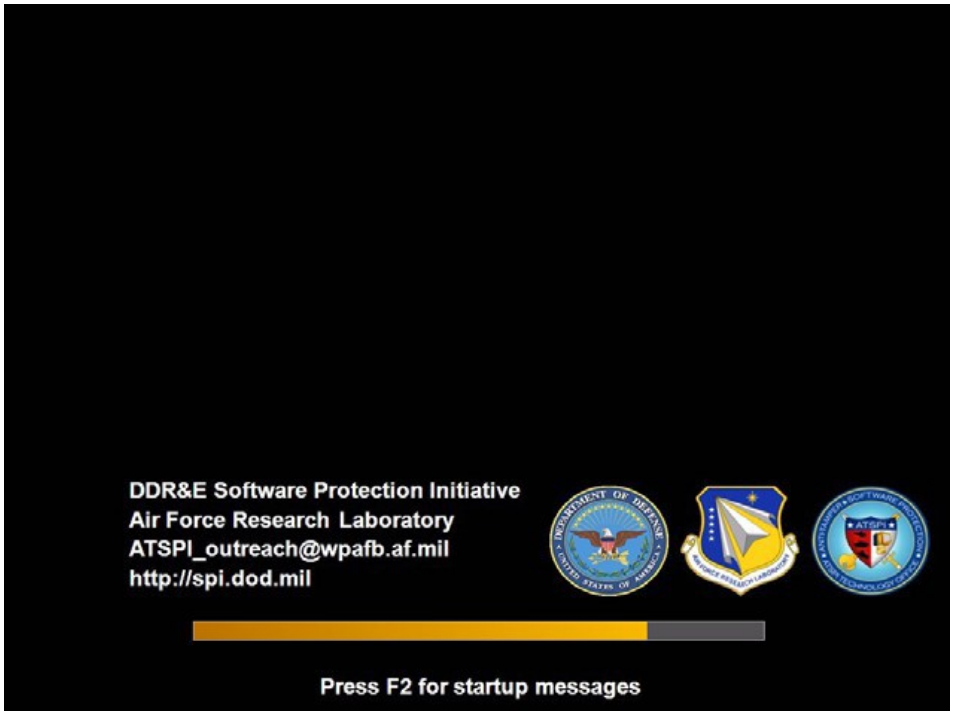
Reiniciar el equipo.

Este deberá arrancar utilizando el CD del "sistema LPS".

nota: si no fuera así, reiniciar de nuevo y preprarar la BIOS del equipo para que arranque desde CD.

Esperar a que el "sistema LPS" se cargue. El proceso de carga es el que aquí se muestra:





Aceptar las condiciones de uso:

Escritorio del "sistema LPS":

Para un acceso seguro a Internet utilizar Firefox (cuyo icono se encontrará arriba a la izquierda):

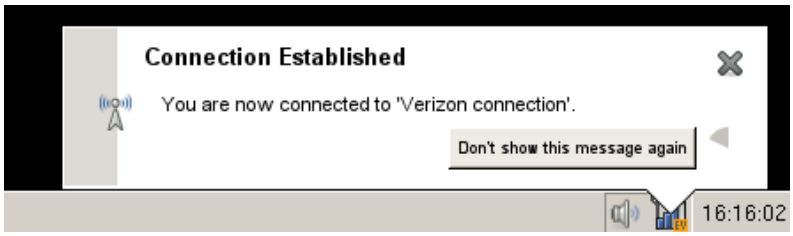
Se recomienda su uso únicamente para el acceso a la páginas web de los bancos o para actuaciones en las que sea necesario introducir datos de tarjetas de débito/crédito u otros datos sensibles.

Conectarse a Internet desde el "sistema LPS"

Si el ordenador está conectado por cable a un router con una conexión activa a Internet, esta se establecerá de forma automática:

Así, se podrá observar, en la esquina inferior derecha, lo siguiente:

y durante unos segundos:



Pero, en el caso de usar una **red WiFi**, se deberá establecer la conexión manualmente:

- Seleccionando la red:

- Introduciendo la contraseña correspondiente:

Tras introducir la contraseña de acceso a la red WiFi, se podrá observar:

- **¿Cuales son los bancos más seguros? Comparativa de páginas web de bancos.**

	Https	Certificado	Teclado Virtual	Olvido de claves (ir a oficina)
BBVA	Si	Si	No	Si
La Caixa	Si	Si	No	No
Popular	Si	Si	No	No
Sabadell	Si	Si	No	
Santander	Si	Si	Si * (existe pero no obliga a usarlo)	No
Ibercaja	Si	Si	Si*(existe pero no obliga a usarlo)	Si
Triodos	Si	Si	Si*(existe pero no obliga a usarlo)	No
Bankia	Si	Si	Si	Si
Deutsche Bank	Si	Si	Si	
Evo	Si	Si	Si	Si
Ing	Si	Si	Si	Si
Ibercaja	Si	Si	Si*	Si
Kutxabank	Si	Si	Si	Si
Unicaja	Si	Si	Si	

Como podemos ver en la tabla todos los bancos se disponen de conexión por https y certificado para para poder verificar la autenticidad de la página web. Es decir, podemos estar seguros de que estamos comunicándonos con nuestro banco y que la comunicación está encriptada.

Sin embargo, no todos los bancos proporcionan un teclado virtual.
Yo pienso que esto es una falta grave, puesto que, aunque el teclado virtual no es infalible, sí es una medida efectiva para evitar que las contraseñas bancarias sean capturadas por un tipo de virus llamado keylogger.

Por la misma razón, la recuperación de las contraseñas, si se olvidan, se debe realizar personalmente en la oficina de nuestro banco. Es un riesgo que se puedan solicitar claves nuevas por internet, introduciendo más datos personales, puesto que estos datos pueden ser capturados por un keylogger.

	Contraseña firma / tarjeta de coordenadas	Autenticación de dos factores (mensaje al móvil)	Aviso por movimiento de dinero (Servicio de alertas)	Consejos de seguridad
Bankia	Firma	Si	Si	Si
BBVA	Firma	-	Si	Si*
Deutsche Bank	Tarjeta de Coordenadas	-	Si	Si
Evo	Tarjeta de Coordenadas	Si	Si	No*
Ibercaja	Ambas	Si	Si	Si
Ing	Ambas	¿No?	Si* (solo tarjetas)	Si
Kutxabank	Tarjeta de Coordenadas	-	Si	Si
La Caixa	Ambas	Si* (solo tarjetas)	Si	No* (existen pero cuesta buscarlos)
Popular	Firma	-	Si	Si
Santander	Firma	-		Si
Sabadell	Tarjeta de Coordenadas	Si	Si	Si
Triodos	Tarjeta de Coordenadas	Si	Si	Si
Unicaja	Tarjeta de Coordenadas	Si	Si	Si

En esta página, las caracteristicas son menos esenciales para la seguridad, aunque también son útiles.

Casi todos los bancos incluyen consejos de seguridad en sus páginas web, y ofrecen el servicio de alertas, mediante mensajes al móvil, ante movimientos de dinero en las cuentas o tarjetas.
Estos servicios son útiles e indican al usuario que está trabajando con un banco que se preocupa por su seguridad.

Así mismo, la mayoría de los bancos, proporcionan una tarjeta de coordenadas a la hora de firmar transferencias u otros cambios. Esto es una cosa positiva, ya que este sistema es superior, en cuanto a seguridad, a la utilización de una única firma.

Por último, algunos bancos, proporcionan la posibilidad de combinar la tarjeta de coordenadas con la autenticación de dos factores (mediante mensaje al móvil de la coordenada).